KANSAS DEPARTMENT OF CORRECTIONS

	INTERNAL MANAGEMENT POLICY AND PROCEDURE	**SECTION NUMBER** **05-110**	**PAGE NUMBER**
		SUBJECT: **INFORMATION TECHNOLOGY AND RECORDS: Security of the Management Information System**	

The IMPP has been placed on RESERVE status, reason being is that the viable content of this IMPP has been subsumed within the parameters of IMPP (05-143) being issued at this time.

Secretary of Corrections

06-02-04
Date

INTERNAL MANAGEMENT POLICY & PROCEDURES

STATEMENT OF ANNUAL REVIEW

IMPP # 05-110

Title: INFORMATION TECHNOLOGY AND RECORDS: Security of the Management Information System

The above referenced Internal Management Policy and Procedure (IMPP), issued effective 05-21-01, was reviewed during January 2004 by the KDOC Policy Review Panel per IMPP 01-101. At the time of this annual review the Policy Review Panel determined that: no substantive changes and/or modifications to this IMPP are necessary at this time, and the IMPP shall remain in effect as issued on the above stated date..

The next scheduled review for this IMPP is January 2005.

This statement of annual review shall be placed in front of the referenced IMPP in all manuals.

_____ _____

Norman Bacon, IT Acting Director — Date
Policy Review Committee Chairperson

_____ 02-03-04

Roger Werholtz, Secretary of Corrections — Date

INTERNAL MANAGEMENT POLICY & PROCEDURES

STATEMENT OF ANNUAL REVIEW

IMPP # 05-110

Title: INFORMATION TECHNOLOGY AND RECORDS: Security of the Management Information System

The above referenced Internal Management Policy and Procedure (IMPP), issued effective 05-21-01, was reviewed during January 2003 by the KDOC Policy Review Panel per IMPP 01-101. At the time of this annual review the Policy Review Panel determined that: some substantive changes and/or modifications to this IMPP may be necessary, but that the specifics of any such revisions are not clear at this time. Although revisions may be forthcoming, the IMPP shall nevertheless remain in effect as issued on the above stated date.

The next scheduled review for this IMPP is January 2004.

This statement of annual review shall be placed in front of the referenced IMPP in all manuals.

_____ _____

Carlos Usera, Information Resource Manager — Date
Policy Review Committee Chairperson

_____ 2-14-03

Roger Werholtz, Secretary of Corrections — Date

INTERNAL MANAGEMENT POLICY & PROCEDURES

STATEMENT OF ANNUAL REVIEW

IMPP # 05-110

Title: INFORMATION TECHNOLOGY AND RECORDS: Security of the Management Information System

The above referenced Internal Management Policy and Procedure (IMPP), issued effective 05-21-01, was reviewed during January 2002 by the KDOC Policy Review Panel per IMPP 01-101. At the time of this annual review the Policy Review Panel determined that: no substantive changes and/or modifications to this IMPP are necessary at this time, and the IMPP shall remaining effect as issued on the above stated date.

The next scheduled review for this IMPP is January 2003.

This statement of annual review shall be placed in front of the referenced IMPP in all manuals.

_____ _____

Carlos Usera, Information Resource Manager — Date
Policy Review Committee Chairperson

_____ 02-05-02

Charles E. Simmons, Secretary of Corrections — Date

KANSAS DEPARTMENT OF CORRECTIONS

	INTERNAL MANAGEMENT POLICY AND PROCEDURE	**SECTION NUMBER** **05-110**	**PAGE NUMBER** **1 of 4**
		SUBJECT: **INFORMATION TECHNOLOGY AND RECORDS: Security of the Management Information System**	
Approved By: **Secretary of Corrections**		**Original Date Issued:**	**01-17-83**
		Current Amendment Effective:	**05-21-01**
		Replaces Amendment Issued:	**06-07-99**

POLICY

Data maintained in the Management Information System shall be safeguarded from unauthorized and improper disclosure. Access to the Department's Management Information System shall be limited to persons properly designated by their appointing authority. All staff that has access to information contained in or produced by the automated Management Information System shall receive training in and be responsive to the security requirements established by the Information Resource Manager.

To ensure a secure repository of automated records and departmental information and to guard against unauthorized and improper access, passwords for designated individuals authorized access to the information system shall be changed in accordance with a schedule and procedures established by the Information Resource Manager.

DEFINITIONS

Appointing Authority: As defined in IMPP 02-109, any person or group of persons empowered by the constitution, by statute, or by lawfully delegated authority to make appointments to positions in the State service pursuant to KAR 1-2-9. Anytime this term is used in this IMPP, it can be read as referring to the "appointing authority or designee".

Information Resource Manager: The position responsible for the development and maintenance of security measures for the computerized Management Information System.

Keylock Security: Access to a terminal linked to the computerized information system that is controlled by a lock and key on the terminal.

Management Information System: A collection of computerized databases that contain information on offenders, which are shared by users of on-line retrieval and hard-copy reports.

Menu Security: Access to menus within the computerized information system that is defined by the Information Resource Manager or designee and controlled by a person's password.

Password: A unique word or combination of letters assigned to a specific employee for the purpose of accessing the computerized information system.

Program Security: Access to programs within menus of the computerized information system that is defined by the Information Resource Manager or designee and controlled by a person's password.

PROCEDURES

I. Security Responsibilities and Requirements

A. The Information Resource Manager shall be responsible for the security of the computerized Management Information System.

B. The Information Resource Manager shall be responsible for assigning or removing the passwords of persons specified by designating authorities.

1. Instructions describing the procedures required for persons authorized access to the Management Information System to receive and verify new passwords shall periodically be distributed to such authorized users by the Information Resource Manager.

C. Persons assigned a password for access to the computerized information system shall be prohibited from disclosing their password to others.

D. No person shall use the computerized Management Information System unless signed on with his/her own password, nor shall they leave the terminal unattended without signing off.

E. Keylock security, password security, menu security, and program security shall be employed at the direction of the Information Resource Manager.

II. Requesting, Removing, or Maintenance of Passwords or Printout Material

A. Requesting Passwords

1. Upon verification that an employee requires access to the computerized Management Information System, the appointing authority shall submit a Management Information System User Agreement Form (Attachment A, Part I, Form #05-110-001) and a Management Information System Access Data form (Part II of Attachment A) to the Information Resource Manager for the employee.

a. The Secretary shall request access for personnel reporting directly to him/her.

b. The division heads shall request access for Central Office staff in their division.

c. The wardens shall request access for personnel in their facility.

d. The regional parole directors shall request access for parole personnel in the regional parole offices.

e. The Access Data form (Part II of Attachment A) shall be completed by the employee's immediate supervisor and submitted to the Information Resource Manager through the appointing authority.

(1) The completed form shall specify the menu(s) needed, the employee's printer identification (if a printer is necessary), and indicate whether the access will require display only, or both display and update capabilities.

2. The assigned password shall be communicated only to the employee to that it was issued along with training/orientation to the security requirements.

   a. This communication shall be by telephone, written document, or in person.

3. Upon issuance, the Information Resource Manager shall advise the requesting official that the password has been issued.

B. Requesting Removal of Passwords or Printout Material

1. The password for a person who no longer requires access, due to reassignment of responsibilities or termination of employment with the Department shall be removed from the computer Management Information System no later than seven (7) calendar days after reassignment or termination. At the time passwords are removed, any printout the person was receiving shall be discontinued automatically.

   a. A removal request shall be made via E-mail by the terminated or reassigned employee's supervisor and sent directly to the Help Desk.

C. Maintenance of Passwords and Staff Authorized Access to the Management Information System

1. The Information Resource Manager shall prepare a listing of those persons having an assigned password.

   a. This listing shall be broken down by facility, parole region, and Central Office work unit or section.

   b. This list shall be compiled on an annual basis each August.

   c. A copy of this list shall be distributed to the appointing authorities.

   d. Each appointing authority shall advise the Information Resource Manager of any errors on the list which need to be corrected.

III. Security and Disposal of Computerized Information

A. Computerized information shall be distributed to those persons demonstrating a need for such information. All computerized information is intended for use by Departmental personnel. Any computerized information for other use (such as contracted services) must be approved by the Information Resource Manager.

B. In order to secure the privacy of offenders, all computerized information or hard copy shall be deleted or shredded when obsolete.

C. Computerized information relating to staff shall be disseminated in accordance with personnel policies and procedures, regulations, and statutes.

D. Computerized information or hard copy containing information on individual offenders, other than name, sentence data, parole eligibility date, disciplinary record, custody level, and physical location, shall be secured in a lockable cabinet or container when not in use.

E. Users of the Management Information System shall not disseminate information to unauthorized parties.

NOTE: The policy and procedures set forth herein are intended to establish directives and guidelines for staff and offenders and those entities who are contractually bound to adhere to them. They are not intended to establish State created liberty interests for employees or offenders, or an independent duty owed by the Department of Corrections to either employees, offenders, or third parties. This policy and procedure is not intended to establish or create new constitutional rights or to enlarge or expand upon existing constitutional rights or duties.

REPORTS REQUIRED

None.

REFERENCES

KSA 45-221(a)(29)
IMPP 01-125
ACO 2-1E-01, 2-1E-06, 2-1E-08, 2-1F-06
ACI 3-4098
APPFS 3-3111

ATTACHMENTS

Attachment A - Part I - Management Information System User Agreement
Part II - Management Information System Access Data, 1 page

Kansas Department of Corrections

Management Information System
Part 1 – User Agreement

I, _____ (please print), have read, understand and agree to comply with all provisions in IMPP 05-110, Security of the Management Information System. The information accessible through and/or from the Management Information system is confidential; therefore, access to this system shall be restricted to those staff approved by the appointing authority.

_____ _____
User Signature Date

_____ _____
Appointing Authority Date

Management Information System
Part II – Access Data

DATE: _____

TO: _____, KS Dept. of Corrections, Information Resource Manager

FROM: _____

SUBJECT: Request Access to _____ TOADS
_____ KDOC MIS
_____ BOTH

Name of Employee: _____ Title: _____

Facility/Office/Unit: _____ Section: _____

Phone #: _____

PO # _____

Please give the full name/title/officer # of the officer whose case load you now have (if applicable)
_____

For MIS, name of MENU needed: _____

If the name of the MENU is not known, please give the full name/title of an existing Management Information System user who has access to the needed MENU: _____
_____

Printer ID: _____ (if a printer is to be used)

Display and/or Update Capabilities Needed (mark one, if applicable) _____ Display Only
_____ Display and Update

APPROVED BY:

_____ _____
Appointing Authority Date

Form #05-110-001